

M. Devlin

UNITED STATES DISTRICT COURT

for the

Western District of Texas

FILED

2012 MAR 15 PM 2:22

CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXASUnited States of America
v.

Case No.

1:12-m-163

BY

DEPUTY

HIGINIO O. OCHOA, III

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 2012 in the county of Travis in the
Western District of Texas, the defendant(s) violated:

Code Section

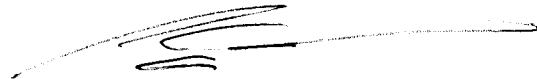
Offense Description

18 U.S.C. § 1030 (a)(5)(A)

Unauthorized access to a protected computer

This criminal complaint is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

Complainant's signature

SCOTT JENSEN, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: March 15, 2012

Judge's signature

City and state: Austin, Texas

Dennis G. Green U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED

2012 MAR 15 PM 2:22

CLERK US DISTRICT COURT
WESTERN DISTRICT OF TEXAS

BY
DEPUTY

SEALED

UNITED STATES OF AMERICA,

Plaintiff,

v.

HIGINIO O. OCHOA III

Defendant.

CRIMINAL NO. 1:12-m-163

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Scott Jensen, being duly sworn, depose and state as follows:

1. I make this affidavit in support of a criminal complaint against HIGINIO O. OCHOA III, year of birth 1981, for violations of Title 18 U.S.C. § 1030 (a)(5)(A) (Unauthorized access to a protected computer).
2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since October 2005. I am currently assigned to the San Antonio Division, Austin Resident Agency. I am assigned to a Cyber Squad where I am responsible for investigating all manner of computer and internet related crime including investigating persons suspected of violating Title 18 U.S.C. § 1030.
3. This affidavit is based on my personal knowledge as well as reports made by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of the complaint, it does not contain every fact known to me or other agents of the Federal Bureau of Investigation.

STATUTORY AUTHORITY

4. Title 18 U.S.C. § 1030 (a)(5)(A) states, in relevant part:

Whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

FACTS

5. On February 7, 2012 at 6:13 PM, Twitter user @Anonw0rmer posted, "@MissAnonFatale I managed to pwn¹ a site , get my papers , find my required primary IDS , yeah baby , i deserves em :)". The West Virginia Chiefs of Police website www.wvcop.com was compromised beginning on February 5, 2012 at 7:37 PM. During this attack the individual(s) gained unauthorized access to the website of the West Virginia Chiefs of Police, and obtained the entire user database. This database contained usernames and passwords for approximately 150 Law Enforcement officials in the state of West Virginia. It also contained the home addresses, home telephone numbers, cellular telephone numbers, and other information for a portion of the 150 officials. This information was then released on the internet. Two officials received harassing and threatening phone calls shortly after the information was released.
6. On February 8, 2012 1:17 AM, Twitter user @Anonwormer posted, "ROFL! WaS that us ? <http://wvgazette.com/News/201202070284> o yeah oops #OpPigRoast #CabinCr3w" An article in the Charleston, WV Gazette discusses the intrusion of www.wvcop.com which is the West Virginia Chiefs of Police website. CabinCr3w is a group of hackers who work together and plan their attacks together under the banner of Anonymous. Anonymous is a loosely affiliated group of hacktivists.
7. Also on February 8, 2012 at 12:31 PM, Twitter user @Anonw0rmer posted, "#Fbi bit.ly/x0uNDN In case your intel guys are staying up too late , let me save you time. #Come #At #ME #bro". This link takes you to an animation showing someone going to www.google.com and typing in CabinCr3w hacks, then pressing the search button.
8. On February 9, 2012 at 12:35 AM, Twitter user @Anonw0rmer posted, "DB Leak <http://dps.alabama.gov> |<http://pastehtml.com/view/bnik8yo1q.html> |" The pastehtml.com link is a website with information stating "CabinCr3w is proud to present: Release: dps.alabama.gov, Credit warmer @cabincr3w" Following that information there is a list of

¹ "pwn" is a common term used in the hacker community for gaining complete access to a server or website.

database table names that are in the Alabama Department of Public Safety database including National Crime Information Center information. The website also contains samples of the information contained in the database including vehicle information, sex offender registrant's information including vehicles, and other personally identifiable information. At the bottom of the website is a picture that shows a female, from the neck down in a bikini top with a sign pinned to her skirt which reads, "PwNd by w0rmer & CabinCr3w <3 u BiTch's!". EXiF² data from this picture shows that it was taken with an iPhone 4 and edited with Photoshop. It also contained GPS coordinates of Latitude: 37 deg 51' 25.20" S, Longitude: 145 deg 15' 1.20" E, Position: 37 deg 51' 25.20" S, 145 deg 15' 1.20" E. Open source research conducted at <http://www.findlatitudeandlongitude.com>, suggests an address of 37 St Clair Rd, Wantirna South VIC 3152, Australia Latitude:-37.856962° Longitude:145.250343°.

9. On February 9, 2012 at 8:42 PM, Twitter user @Anonw0rmer posted, "Mobile Alabama Police | Criminal Record Database| Logins | Failing To Protect And Serve | Via @ItsKahuna |<http://pastehtml.com/view/bnmjxxgfp.html> #OpPiggyBank. This website contains a statement about "oppression by police departments around the world...EVERY police department is at risk and will remain that way..." There was also another link www.pastebay.net/307542 which contained data taken from the Mobile Police Department servers.
10. On February 9, 2012 at 8:39 PM, Twitter user @CabinCr3w posted, "Texas Dept. of safety Hacked By @AnonW0rmer for #OpPiggyBank<http://bit.ly/x1KH5Y> #CabinCr3w #Anonymous (link not broken)" The shortened url <http://bit.ly/x1KH5Y> leads you to pastehtml.com/view/bnm8z2mlq.html. This site states, "CabinCr3w is proud to present Release: www.txdps.state.tx.us Credit: w0rmer@cabinCr3w". It also had a list of table names from the DPS database including a sample of data from these tables. At the bottom there was a picture of a female with a sign stating "We Are ALL Anonymous We NEVER Forgive. We NEVER Forget. <3 @Anonw0rmer". This picture appears to be the same female that was depicted in the Alabama DPS release.

² Exchangeable image file format (Exif) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. This data can include what type of device was used, what settings were used and location information.

11. A review of log files from the Texas DPS website revealed that it had been compromised on February 8, 2012 at 16:12 CST by IP address 108.87.86.190 utilizing a SQL injection vulnerability that allowed the attacker to gain unauthorized access to server resources including tables on a database utilized by the webserver. This access allowed the attacker to create and drop database tables as well as download data, all functions that were not intended. An administrative subpoena served upon AT&T Internet Services revealed that IP address 108.87.86.190, at the time of the attack, was assigned to Erin Beltramini at 4925 Ft. Crockett Boulevard, Apartment #325, Galveston, TX 77551.
12. On February 10, 2012 at 9:07 PM, Twitter user @Anonw0rmer posted, "My baby SETS standards ! wAt U g0t? | <http://i.imgur.com/FbH2K.jpg> | <http://i.imgur.com/zsPvm.jpg> | <http://i.imgur.com/S2S2C.jpg> | <http://i.imgur.com/TVqdN.jpg> | #CabinCr3w". The i.imgur.com websites all lead to images of what appears to be the same female in pictures associated with the TX DPS and Alabama DPS compromises. These pictures also reference w0rmer and @Anonw0rmer along with CabinCr3w. The links in the post show images of a female in various states of undress holding various signs. One of the pictures is the same as the Alabama DPS picture with the EXiF data that shows it was taken in Australia.
13. On February 11, 2012 11:42 AM, Twitter user @Anonw0rmer posted, "To my #Fed Followers! | <http://i.imgur.com/nbED2.jpg> |". This picture shows the same female with a sign stating "Come @ me bro! @Anonw0rmer #Cabincr3w".
14. On February 20, 2012 at 2:14 AM, Twitter user @Anonw0rmer posted, "HACKED: <http://www.houstoncounty.org> | Do u see it ?<http://www.houstoncounty.org/dept.php?id=12> | TEASER:<http://www.houstoncounty.org/dept.php?id=12&page=11> | @Anonw0rmer @CabinCr3w #CabinCr3w". On February 20, 2012 at 3:09 AM, Twitter user @Anonw0rmer posted, "DEFACE: <http://www.houstoncounty.org> By @Anonw0rmer <3 @CabinCr3w #CabinCr3w". On February 20, 2012 at 10:27 AM, Twitter user @Anonw0rmer posted, "<http://www.houstoncounty.org/> | TANGO:DOWN | What no admin accounts to fix deface IT team ? weak!". On February 20, 2012 at 10:56 AM, Twitter user @Anonw0rmer posted, "@RadnusJ yer , i pwnd all of houston countys datebase haaha". On February 20, 2012 at 10:57 AM, Twitter user @Anonw0rmer posted, "@memoryne rofl they had to take it offline because i deleted all the admin accounts...but mine haaha".

15. On February 20, 2012 Houston County in Alabama experienced a website defacement. In addition the attacker created fake events on their online calendar, posted images representing Anonymous and CabinCr3w, deleted all the administrator accounts except the one created by the attacker. All of this was accomplished by gaining unauthorized administrator access to the site's control panel. The county was forced to take their website down and rebuild the website from backups since they had no way to gain access to their website to fix the issues that the hacker created.
16. On February 12, 2012 at 4:54 AM, Twitter user @Anonw0rmer posted, "pWND! Me & @s3rverexe Playing with bots ! This is what happens when you kill the wrong process LULZ!mg580.imageshack.us/img580/6416/ca...". This picture shows a screenshot of a computer desktop. On the desktop are a number of open, running programs with an error message in front of them. There is a window showing Skype running with a username of anonw0rmer logged in. There is another program running called KVIrc version 4. In this window, the username @higochoa is logged in.
17. An open source search for the username w0rmer revealed two posts on the website <http://search.gmane.org/?author=oO+W0rMeR+Oo&sort=date>. One post states, "I just signed up and am waiting to jump right in im a Visual Basic Programmer and network admin, so im ready for the challenge, cant wait. Any VB Programers please send me some info regarding the syntax to the commands for the servers" and is signed "-Higino Ochoa AkA w0rmer".
18. A Texas Department of Motor Vehicles search brings up a Drivers License for Higinio Ochoa with the following information:
Higinio O Ochoa III
DL in TX # 24537042
6424 Central City Bl #828
Galveston, TX 77551
Date of Birth 07/23/1981
19. A open source search for @Higochoa revealed the website <http://www.geocaching.com/seek/log.aspx?LUID=b706f1f1-1688-44b7-8fbf-209cead1a0d2&IID=38063323-98b9-4469-95cc-fae50b4f7158> which showed a picture of an

individual that was geocaching in Texas. The picture appears to be of Higinio Ochoa based on a comparison to the DL photo of Higinio O Ochoa III.

20. On Feb 5th, 2012 at 10:53 PM, Twitter account @higochoa posted, "LEAK: #OpPiggyBank West Virginia wvcop.com tinyurl.com/6tvokka By #W0rmer @CabinCr3w @ItsKahuna #Anonymous #CabinCr3w". At this time, the twitter account @Anonw0rmer did not exist. On February 6, 2012 at 11:18 AM, @Anonw0rmer posted their first Twitter post. The first account login associated with the Twitter account is from the Czech Republic. This is consistent with other intrusion records showing IP addresses located in various foreign countries, which is consistent with someone trying to hide their true IP address. The second login is from IP address 98.199.27.132, which is controlled by Comcast Communications in Houston, TX.
21. On March 2, 2012 it was learned that address 6424 Central City Bl #828 Galveston, TX 77551 was no longer in use by Ochoa. Ochoa broke the lease in 2010 and left a forwarding address of 4925 Fort Crockett Blvd. # 313 Galveston, TX 22551. This apartment is one floor down, and one apartment over from Erin Beltamini's address of 4925 Ft. Crockett Boulevard, Apartment #325, Galveston TX 77551. Due to the proximity of the two addresses, it is likely that Ochoa used his neighbor's unsecured wireless network to perform the intrusion on the Texas Department of Public Safety servers.
22. Surveillance conducted on March 3 – 4, 2012 revealed that Ochoa is living at 4925 Fort Crockett Blvd, #313, Galveston, TX 22551.
23. A Facebook profile was located for Higinio Ochoa and can be found at www.facebook.com/galvestonman. According to this Facebook profile, Ochoa is residing in the Galveston, TX area. On his Facebook profile it states that he is in a relationship with Kylie Gardner. Kylie Gardner's Facebook profile which can be found at <http://www.facebook.com/kyliegardner>, states that she graduated from Dungog High School which is located in Dungog, New South Wales, Australia. The EXiF data from the first picture posted on the profile shows it was taken in Australia.
24. Further open source searches revealed a LinkedIn.com³ profile for Higinio Ochoa listing him as the Lead Administrator for Bombshellnet.org in Houston, Texas. Bombshellnet.org is a now defunct free linux shell service.

³ LinkedIn.com is a business related social networking site

CONCLUSION

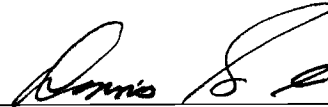
25. Based upon the above information there is probable cause to believe that Higinio O. Ochoa III has committed the offenses set forth in the attached Criminal Complaint.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



SCOTT JENSEN
Special Agent
Federal Bureau of Investigation
Austin, Texas

Subscribed and sworn to before me at Austin, Texas, on this 15th day of March, 2012.



UNITED STATES MAGISTRATE JUDGE